



شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكرو فيلم

بسم الله الرحمن الرحيم



MONA MAGHRABY



شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم



شبكة المعلومات الجامعية التوثيق الإلكتروني والميكروفيلم



MONA MAGHRABY



شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات



يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار



MONA MAGHRABY



**AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING**

Electronics and Electrical Communication Department

**Physical Unclonable Function (PUF) Design
for IoT Applications**

**A dissertation submitted to ASU in partial fulfillment of
the requirements for the award of the degree of**

**Doctor of Philosophy
in
Electronics and Communication Engineering**

By

Eng. Amin Amin Sayed Zayed

Supervised by

Prof. Hani Fikry

Prof. Khaled Shehata

Prof. Hanady H. Issa

Electronics and Electrical
Communication Department
Faculty of Engineering
Ain Shams University
Cairo, Egypt

Electronics
& Communications
Engineering Department
AASTMT
Cairo, Egypt

Electronics
& Communications
Engineering Department
AASTMT
Cairo, Egypt

**CAIRO
2021**



AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING

Physical Unclonable Function (PUF) Design for IoT Applications

By

Amin Amin Sayed Zayed

Doctor of Philosophy in Electrical Engineering
(Electronics and Communications Engineering)

Examiners' Committee

Name and Affiliation

Signature

Prof. Amr Mamdouh Bayoumi
Zewail City of Science and Technology

.....

Prof. Mohamed Amin Dessouky
Faculty of Engineering
Ain Shams University.

.....

Prof. Hani Fikry Ragaai
Faculty of Engineering
Ain Shams University.

.....

Prof. Hanady Hussein Issa
Arab Academy for Science,
Technology and Maritime Transport.

.....

Date: 19 June 2021

ACKNOWLEDGMENT

My deepest appreciation goes to my supervisors **Prof. Hani Fikry, Prof. Khaled Shehata, and Prof. Hanady Hussein**. I would like to thank them all for their continuous guidance, support and active contribution in refining my research work.

ABSTRACT

Physical Unclonable Functions (PUFs) are promising hardware security primitives that are based on the uniqueness and the unclonability of the device's physical characteristics to provide a unique identifier for devices. PUFs are suitable for low power applications, such as the Internet of Thing (IoT). PUFs can be used in device authentication and for secure key storage and generation. The Ring Oscillator (RO) PUF is one of the most reliable and strong PUFs. On the other hand, it consumes more power than others. The main aim of this thesis is to propose a design for a low power PUF. In this thesis we propose three new PUFs architectures, which are suitable for low power applications. The three proposed PUFs were designed using 20 nm triple gate FinFET technology.

The first proposed design presents a Frequency Divider Ring Oscillator PUF (FDRO-PUF). The FDRO-PUF design is based on utilizing modules that consume less power than the conventional one. In the FDRO-PUF design the Frequency Divider (FD) and the D-flipflop (DFF) are employed instead of the counters, the timer, and the comparator circuits. Evaluation results demonstrate that the FDRO-PUF design can effectively reduce power consumption. The FDRO-PUF consumes 264 μW per challenge-response pair at supply voltage 0.9 V. The averaged reliability of the proposed design is 99.5 %, over a range of temperature from -40 to 125 $^{\circ}\text{C}$ and supply voltage from 0.8 V to 1 V.

The second proposed design presents Edge Detector Ring Oscillator PUF (EDRO-PUF). The EDRO-PUF design is based on biasing the ROs near the threshold voltage to reduce the consumption power. In the EDRO-PUF design the FD and the Edge Detector (ED) replaced the counters, the timer, and the comparator circuits. Simulation results demonstrate that the EDRO-PUF design can effectively reduce power consumption. The Simulation results for 1000 different chips with the same input challenge, show that the average power is 2.2 μW , at supply voltage 0.5 V. The average reliability of the EDRO-PUF is 99.1%, at temperatures from -40 to 125 $^{\circ}\text{C}$ and supply voltage $0.5 \pm 10\%$.

The third proposed design presents Oscillator Collapse Physical Unclonable Function (OC-PUF). The power consumption is reduced based on designing the most power-hungry modules in the OC-PUF. An Oscillator Collapse (OC) is designed to work in the near-threshold voltage region reducing power consumption. More power reduction is achieved by designing a new Collapse Time Comparator (CTC). Due to the process variations, the oscillation period

of each OC is different. The CTC generates the output response bit by comparing the oscillation periods of the two selected OCs. The simulation results demonstrate that the proposed OC-PUF can effectively reduce the power consumption. The Simulation results for 1000 different chips with the same input challenge, show that the average power is 140 nW, with the worst case being 740 nW. The best case is 63 nW per challenge-response pair at supply voltage 0.5 V. The average reliability of the OC-PUF is 99.8%, at temperatures from -40 to 125 °C and supply voltage $0.5 \pm 10\%$. The three proposed PUFs decrease the power consumption while retaining high-performance metrics.

TABLE OF CONTENTS

LIST OF TABLES.....	X
LIST OF ABBREVIATIONS.....	XI
LIST OF PUBLICATIONS.....	XII
1 INTRODUCTION.....	1
1.1 LITERATURE REVIEW.....	1
1.2 THESIS OBJECTIVE.....	3
1.3 THESIS OUTLINE.....	3
2 PHYSICAL UNCLONABLE FUNCTIONS.....	5
2.1 PUF CLASSIFICATION.....	6
2.1.1 Electronic and Non-electronic PUFs.....	6
2.1.2 Intrinsic and Non-intrinsic PUFs.....	7
2.1.3 Weak and Strong PUFs.....	8
2.2 PUF ARCHITECTURE.....	8
2.2.1 Arbiter PUF.....	8
2.2.2 Ring Oscillator PUF.....	11
2.2.3 Transient Effect Ring Oscillators PUF (TERO-PUF).....	12
2.2.4 SRAM PUF.....	14
2.2.5 Butterfly PUF.....	15
2.2.6 Optical PUF.....	16
2.2.7 Coating PUF.....	17
2.3 APPLICATIONS OF PUF.....	18
2.3.1 Device Identification.....	18
2.3.2 Authentication.....	19
2.3.3 Cryptographic Key Generation.....	20
2.4 PERFORMANCE METRICS.....	21
2.4.1 Uniqueness.....	21
2.4.2 Reliability.....	21
2.4.3 Uniformity.....	22

3	FREQUENCY DIVIDER RING OSCILLATOR PUF.....	23
3.1	PROPOSED FREQUENCY DIVIDER RO-PUF	23
3.1.1	Proposed Nine Stage Ring Oscillator	25
3.1.2	D Flip-Flop (DFF)	26
3.1.3	Frequency Divider	27
3.1.4	Multiplexer	29
3.2	SIMULATION RESULTS AND COMPARISON	31
3.2.1	Threshold Voltage	32
3.2.2	Average Power of the Ring Oscillator	33
3.2.3	D flip-flop Response Time	36
3.2.4	Number of Stages of the Frequency Divider	37
3.2.5	Uniqueness	38
3.2.6	Reliability	39
3.2.7	Uniformity	40
3.2.8	Power Analysis	40
4	EDGE DETECTOR RING OSCILLATOR PUF	41
4.1	SCALING THE INVERTER SUPPLY VOLTAGE	41
4.2	PROPOSED EDGE DETECTOR RO-PUF	42
4.2.1	Proposed Seven Stage Ring Oscillator	43
4.2.2	Edge Detector (ED)	44
4.2.3	Demultiplexer	46
4.2.4	Frequency Divider	47
4.2.5	Multiplexer	47
4.2.6	OR Gate	47
4.3	SIMULATION RESULTS AND COMPARISON	48
4.3.1	Ring Oscillator Power Consumption	48
4.3.2	Edge Comparator Response Time	49
4.3.3	Number of Stages of the Frequency Divider	50
4.3.4	Uniqueness	51
4.3.5	Reliability	51
4.3.6	Uniformity	52
4.3.7	Power Analysis	53

5	OSCILLATOR COLLAPSE PUF	54
5.1	PROPOSED OSCILLATOR COLLAPSE PUF DESIGN.....	54
5.1.1	Oscillator Collapse (OC)	56
5.1.2	Collapse Time Comparator (CTC)	59
5.1.3	Multiplexer	63
5.1.4	De-multiplexer.....	63
5.2	SIMULATION RESULTS AND COMPARISON	63
5.2.1	Uniqueness	63
5.2.2	Reliability	64
5.2.3	Uniformity	65
5.2.4	Power Analysis	66
5.2.5	Comparisons	69
6	CONCLUSION AND FUTURE WORK.....	71
6.1	CONCLUSION.....	71
6.2	FUTURE WORK	72
7	REFERENCES	73

LIST OF FIGURES

Figure 2.1: Physical unclonable functions.....	5
Figure 2.2: The A-PUF [49], (a) A-PUF circuit, (b) A-PUF operation.....	9
Figure 2.3: The feed-forward A-PUF [52].	10
Figure 2.4: XOR A-PUF [54].....	10
Figure 2.5: Ring oscillator PUF [6].	11
Figure 2.6: TERO-PUF architecture [56].	12
Figure 2.7: The TERO loop structure [56].	13
Figure 2.8: Behavior of the two TERO loops.....	13
Figure 2.9: SRAM PUF cell [60].	14
Figure 2.10: Butterfly PUF [61].	15
Figure 2.11: Optical PUF [63].....	16
Figure 2.12: Coating PUF [64].....	17
Figure 2.13: Device identification [67].	18
Figure 2.14: Authentication [68].	19
Figure 2.15: Cryptographic keys [70].....	20
Figure 3.1: Basic Ring Oscillator PUF [5]	23
Figure 3.2: Proposed Frequency Divider RO-PUF (FDRO-PUF)	24
Figure 3.3: Proposed nine Stage Ring Oscillator and Bias circuit	25
Figure 3.4: Bias circuit	25
Figure 3.5: DFF circuit [81]	26
Figure 3.6: Simulation results of the DFF circuit.	26
Figure 3.7: Proposed frequency divider.	27
Figure 3.8: TFF circuit [82].....	28
Figure 3.9: Simulation results of the TFF circuit.	28
Figure 3.10: Transmission gate logic Circuit [83].....	29
Figure 3.11: Circuit diagram to 4:1 MUX based TGL [83].	30

Figure 3.12: Simulation results of 4:1 MUX, the MUX's selectors are set to logic '10' to select D1.	30
Figure 3.13: Extracted V_{th} value for nFinFET, from simulation results by the constant current method based on the I_D - V_{GS} characteristics.	32
Figure 3.14: Extracted V_{th} value for pFinFET, from simulation results by the constant current method based on the I_D - V_{GS} characteristics.	33
Figure 3.15: The average power for the proposed RO at different V_c values.	33
Figure 3.16: Proposed ring oscillator output oscillation.	34
Figure 3.17: Histogram for the RO frequency.....	35
Figure 3.18: DFF for the RO frequency.	36
Figure 3.19: Simulation results of the proposed frequency divider (FD) circuit.	37
Figure 3.20: Inter-PUF Hamming Distance.	38
Figure 3.21: Intra-PUF Hamming Distance.	39
Figure 3.22: Uniformity Of FDRO-PUF.	40
Figure 4.1: The proposed Edge Detector RO-PUF (EDRO-PUF)	42
Figure 4.2: Proposed seven stage ring oscillator and a bias circuit.....	43
Figure 4.3: Proposed Edge Detector (ED).....	44
Figure 0.4: Simulation results of the ED circuit.....	45
Figure 4.5: The XOR circuit [92].	45
Figure 4.6: Simulation results of the XOR circuit.....	45
Figure 4.7: Circuit diagram of 1:4 DeMUX based TGL.	46
Figure 4.8: Simulation results of 1:4 DeMUX.	46
Figure 4.9: The OR circuit [89].	47
Figure 4.10: Simulation results of the OR gate.	47
Figure 4.11: Proposed Ring Oscillator output oscillation.	48
Figure 4.12: Simulation of ED, where the ED_OUT is at logic '1'.....	49
Figure 4.13: Simulation of ED, where the ED_OUT is at logic '0'.....	49
Figure 4.14: Proposed Frequency Divider (FD).	50

Figure 4.15: Simulation results of the proposed FD.....	50
Figure 4.16: Inter-PUF Hamming Distance.	51
Figure 4.17: Intra-PUF Hamming Distance.	52
Figure 4.18: Uniformity Of FDRO-PUF.	52
Figure 5.1: Proposed OC-PUF.	55
Figure 5.2: Schematic of (a) the Proposed Oscillator Collapse, (b) Inverter, (c) Bias circuit, and (d) NAND gate.....	57
Figure 5.3: Oscillator collapse simulation output.....	58
Figure 5.4: Charge Pump circuit [96].....	59
Figure 5.5: Charge Pump output signal and the instantaneous power.	60
Figure 5.6: Proposed Collapse Time Comparator (CTC).....	61
Figure 5.7: CTC output signal and its instantaneous power.....	61
Figure 5.8: Frequency distribution of the OC-PUF Inter Hamming Distance.	64
Figure 5.9: Frequency distribution of the OC-PUF Intra Hamming distance.	64
Figure 5.10: Frequency distribution of the OC-PUF Intra Hamming distance, without using capacitors.	65
Figure 4.11 Uniformity of the OC-PUF.	66
Figure 4.12: OT histogram for OC14, which has the maximum OT.....	67
Figure 4.13: The output signal and instantaneous power for OC14, run number 809 from 1000 runs, which has maximum OT.....	67
Figure 4.14: Histogram for the OC-PUF average consumption power.....	69

LIST OF TABLES

Table 3-1: FinFET parameters.....	31
Table 3-2: Proposed RO average power, frequency, amplitude at different Vc values	34
Table 3-3: Ring oscillator Monte Carlo simulations output	35
Table 5-1: Charge Pump and Collapse Time Comparator	62
TABLE 5-2: Performance comparison among proposed OC, conventional OC, and c0nventional RO.....	68
TABLE 5-3: Summary of the simulation results of the three proposed PUFs and comparison with the state-of-the-art strong PUFs.	70